REMARKS

In the Office Action mailed March 18, 2005, the Examiner rejected claims 1-33 under 35 U.S.C. § 103(a) as being obvious in view of *Bisbee* (U.S. Patent No. 6,367,013) in view of *CFSB* (Computer Fraud & Security Bulletin, "How Key Escrow Might Work").

Applicant has amended claims 1-8, 10, 12, 14-17, 19, 21, 26, 28, 30, and 33 and canceled claims 11, 22-24, and 29 without prejudice or disclaimer. Based on these amendments and the following remarks, Applicant respectfully traverses the rejection of claims 1-33 under U.S.C. §103(a).

I. The Rejection of Claims 1-33 Under 35 U.S.C. §103(a)

To establish a prima facie case of obviousness, three basic criteria must be met. First, the prior art reference or references, taken alone or combined, must teach or suggest each and every element recited in the claims. *See* M.P.E.P. § 2143.03. Second, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine the references in a manner resulting in the claimed invention. *See* M.P.E.P. § 2143. Third, a reasonable expectation of success must exist. *See* M.P.E.P. § 2143.02. Moreover, each of these requirements must "be found in the prior art, and not based on applicant's disclosure." M.P.E.P. § 2143.

a. The Cited Art Does Not Support the Recitations of Claims 1-33

The Examiner asserts *Bisbee* teaches a Trusted Custodial Utility (TCU) that stores information objects and digitally signed, authenticated and encrypted documents or information objects. (*See e.g., Office Action*, page. 3, ¶ 2, page 4, ¶4, page 8, ¶ 5) Although the TCU taught by *Bisbee* does store encrypted information objects, *Bisbee* does not disclose or suggest storing a user's encryption key. Indeed, *Bisbee* states that the information maintained by the TCU includes documents or objects that have already been signed by keys or other security mechanisms (*See e.g., Bisbee*, col. 8, lines 40-65 and col. 12, lines 30-42.) Accordingly, *Bisbee* does not support the rejections of claims 1-33, as asserted by the Examner. For example, *Bisbee* does not teach or suggest at least encrypting a user's encryption key with a first archival key and storing the encrypted user's encryption key in a database under the control of a first entity separate from the certificate authority, as recited in claims 1 and 33. Moreover, *Bisbee* does not teach or suggest a data processing system comprises a data recovery manager separate from the certificate authority that receives and manages archiving of the encryption key, and wherein the user's encryption key is encrypted during transmission from the user using the data recovery manager's public transport key, as recited in claim 19.

In addition, the Examiner admits that *Bisbee* does not disclose receiving an indication of proof of archival of the user's encryption key. The examiner cites to *CFSB* to make up for the deficiencies of *Bisbee.* (*See Office Action, page 3.* ¶¶ 3 and 4). In particular, the Examiner asserts *CFSB* discloses receiving an indication of

proof of archival. Although *CFSB* may disclose the use of a escrow certificate to provide proof of a key being escrowed, the reference, alone or in combination with *Bisbee,* does not disclose or suggest the recitations of Applicant's claims. In particular, the Examiner asserts *CFSB* teaches an "indication of proof or archival [that] is digitally signed, and . . . verifying a digital signature on the indication of proof or archival." (*See Office Action,* page 7, ¶ 3.) Applicant disagrees. Although *CFSB* discloses an escrow certificate associated with the escrowing of a key, the reference falls short in describing the verification of a digital signature associated with a proof of archival, as asserted by the Examiner. Moreover, assuming *CFSB* disclosed verifying the escrow certificate — a position Applicant does not concede — the verification would be performed by the certificate authority, which is distinct from Applicant's claims.

For example, the cited art does not teach or suggest at least providing an indication of proof of storing the encrypted user's encryption key, wherein the indication of proof is signed with a second archival key and verifying the signed indication of proof based on the first archival key, and providing the request to the certificate authority based on the verification of the signed indication of proof, as recited in claims 1 and 33. Moreover, *CFSB*, alone or in combination with *Bisbee,* does not disclose or suggest a processor configured to execute program instructions to, among other things, verify an indication of proof and provide a digital certificate request to a certificate authority based on the verification of the indication of proof, as recited in claim 15. Additionally, the cited art fails to teach or suggest, alone or in combination, at least receiving an indication of proof of archival of a user's encryption

key associated with a request, whereby the user's encryption key is archived under control of an entity other than the certificate authority, verifying the indication of proof, and receiving a digital certificate from the certificate authority based on the verified indication of proof, as recited in claim 19.

The cited art also fails to teach or suggest, alone or in combination, "verifying the digitally signed indication of proof; sending a request for a digital certificate based on the verifying; and receiving a digital certificate in response to the request," as recited in claim 10. Further, the cited art fails to teach or suggest, alone or in combination "providing the indication of proof of archival to a second entity that verifies the indication of proof and provides a request for a digital certificate from the certificate authority based on a verified indication of proof," as recited in claims 12 and 30. Moreover, the cited art fails to teach or suggest, a processor configured to execute program instructions to, among other things, verify an indication of proof and provide a digital certificate request to a certificate authority based on the verification of the indication of proof, as recited in claim 15.

Claim 16 recites, among other things, "a processor configured to execute the program instructions to send a request for a digital certificate, the request having a verified indication of proof of archival of an encryption key for the user in an entity separate from the certificate authority, and receive a digital certificate in response to the request." Claim 17 recites, "a processor configured to execute the program instructions to receive an encryption key for archiving, archive the received encryption key, create an indication of proof of archival of the received encryption key, and send the indication of proof of archival to an entity that provides a request

for a digital certificate to the certificate authority based on a verification of the indication of proof of archival." Claim 19 recites a method for requesting a digital certificate from a certificate authority and archiving an encryption key outside of the certificate authority that includes, among other things, "verifying the indication of proof" and "receiving a digital certificate from the certificate authority based on the verified indication of proof." And, claim 28 includes "verifying the digitally signed indication of proof; sending a request for a digital certificate based on the verified digitally signed indication of proof; and receiving a digital certificate in response to the request." The cited art, alone or in combination, fails to teach these recitations.

Accordingly, the cited art that the Examiner relies upon do not support the rejection of claims 1, 10, 12, 15-17, 19, 28, 30, and 33. Based on the foregoing, Applicant requests that the rejection of these claims under 35 U.S.C. § 103(a) be withdrawn, and the claims allowed.

Claims 2-9 depend from claim 1; claims 13 and 14 depend from claim 12; claims 20, 21, and 25-27 depend from claim 19; and claims 31 and 32 depend from claims 30. As explained, the cited art does not support the rejection of claims 1, 12, 19, and 30. Accordingly, the cited art does not support the rejections of claims 2-9, 13, 14, 20, 21, 25-27, and 31 and 32 for at least the same reasons set forth above in connection with claims 1, 12, 19, and 30. As such, Applicant requests that the rejection of these claims be withdrawn and the claims allowed.

The Examiner also asserts that *Bisbee* discloses a registration manager, as recited in claim 18, but fails to disclose sending a user's encryption key and in response receiving an indication of proof of archival. To make up for these

deficiencies, the Examiner asserts *CFSB* discloses an indication of proof of archival associated with a request. (*See Office Action*, page 4, ¶¶ 4-6.) The Examiner also asserts *Bisbee* in combination with *CFSB* discloses a data recovery manager, as recited in claim 18. Applicant disagrees with the Examiner's assertions.

Bisbee discloses a system that includes a certificate authority, a registration authority, and a TCU. The certificate authority implements a repository (DCR) for storing certificates, thus is under control of the certificate authority (*See Fig. 2).* The registration authority may interact with the certificate authority to collect certificates. The TCU, as explained above, stores signed documents or information objects and provides proof of authenticity of these documents for other entities. Contrary to the Examiner's assertions, none of these elements, or any others disclosed by *Bisbee* suggest a registration manager configured to receive a digital certificate request including a user's encryption key, send the user's encryption key, and in response receive an indication of proof of archival. Further, *CFSB* merely describes using an escrow agent to maintain a key and the possible use of escrow certificates, which falls short of describing or suggesting the implementation of a registration manager, as recited in claim 18.

Further, contrary to the Examiner's assertions, the cited art does not disclose or suggest a data recovery manager configured to receive the user's encryption key, send the user's encryption key to a database controlled by an entity other than the certificate authority for archiving, create an indication of proof archival, and send the indication of proof of archival, as recited in claim 18. As explained, the TCU taught by *Bisbee* does not store user encryption keys. Instead, the TCU maintains signed

documents and/or information objects. Further, nowhere does *CFSB* disclose a recovery manager, as recited in claim 18. Indeed, the cited art falls short in describing a system including a data recovery manager that sends an indication of proof and a registration manager that receives the indication of proof. Additionally, the cited art fails to disclose, in addition to the data recovery manager and registration manager, a certificate authority that issues a digital certificate when it is determined that the indication of proof was received. While *CFSB* states a certificate authority would need proof that a key has been escrowed through an escrow certificate, the reference does not disclose a registration manager that receives an indication of proof and a certificate authority that issues a digital certificate when it is determined the indication of proof was received, as recited in claim 18.

Accordingly, the cited art fails to support the rejection of claim 18 under 35 U.S.C. § 103(a) and Applicant requests the rejection be withdrawn and the claim allowed.

b. There is No Motivation to Combine Cited Art as Asserted by the Examiner

Moreover, *prima facie* obviousness has not been established at least because there is no motivation to combine *Bisbee* and *CFSB*. Determinations of obviousness must be supported by evidence in the record. *See In re Zurko*, 258 F.3d 1379, 1386 (Fed. Cir. 2001) (finding that the factual determinations central to the issue of patentability, including conclusions of obviousness by the Board, must be supported by "substantial evidence"). Further, the desire to combine references must be proved with "substantial evidence" that is a result of a "thorough and searching" factual

inquiry. *In re Lee*, 277 F.3d 1338, 1343-1344 (Fed. Cir. 2002) (quoting *McGinley v. Franklin Sports, Inc.*, 262 F.3d 1339, 1351-52).

In this case, the Office Action does not show that a skilled artisan considering *Bisbee* and *CFSB*, and not having the benefit of Applicant's disclosure, would have been motivated to combine or modify the references in a manner resulting in Applicant's claimed combination. In fact, the Examiner merely states a conclusion of the alleged combination without providing the requisite motivation to support the combination. The Examiner alleges that a skilled artisan would have modified *Bisbee.* because "CFSB teaches providing benefits to owners for archiving key especially for the situation even after acquiring the new key pair, data retransmission is not possible (e.g., voice mailbox messages)." (*See Office Action*, pp. 3-4.) This conclusion is not properly supported and does not show that a skilled artisan would have modified the reference as alleged. The mere fact that *CFSB* mentions a key escrow system does not show that a skilled artisan would have been motivated to modify *Bisbee* as alleged.

The M.P.E.P. makes clear that: "[t]he mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination" M.P.E.P. § 2143.01 (citations omitted). The Examiner has not shown that the cited art "suggests the desirability" of the alleged combination. Indeed, there is no reason why a skilled artisan would look to modify *Bisbee* with *CFSB.* For example, the TCU taught by *Bisbee* has no need for a key escrow agent because it maintains already signed documented and information objects. Further, the certificate authority itself maintains

a repository of certificates (DCR), thus having a key escrow agent for these certificates is not needed. Therefore the conclusions in the Office Action were not reached based on facts gleaned from the cited references and that, instead, teachings of the present application were improperly used in hindsight to reconstruct the prior art. For at least these additional reasons, the Examiner has not established a *prima facie* case of obviousness with respect to claims 1-33, and thus, the rejection of these claims under 35 U.S.C. § 103(a) should be withdrawn and the claims allowed.

II. Conclusion

In view of the foregoing remarks, Applicant submits that this claimed invention, is neither anticipated nor rendered obvious in view of the cited art. Applicant therefore requests the Examiner's reconsideration and reexamination of the application and the timely allowance of claims 1-33.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: June 17, 2005

By: _____
Joseph E. Palys
Reg. No. 46,508